Performance Analysis of GNSS Spoofing Mitigation Techniques based on Array Antennas in Various Spoofing Scenarios

J. H. Noh, B. H. Gong, Y. S. Lee, B. C. Jung, S. J. Lee
Department of Electronic Engineering, Chungnam National University, Republic of Korea

H. H. Choi
Satellite Navigation Team, Korea Aerospace Research Institute, Republic of Korea

BIOGRAPHY (IES)

Jae Hee Noh is a Ph.D candidate with the Department of Electronics Engineering at Chungnam National University in Korea. She received B.S and M.S degrees from Chungnam National University, Department of Electronic Engineering in 2017 and 2019, respectively. Her research interests include GNSS receiver, anti-spoofing techniques and message authentication.

Heonho Choi is a senior researcher with the Division of satellite navigation R&D at Korea Aerospace Research Institute. He received M.S and Ph. D degrees from Chungnam National University, Department of Electronic Engineering in 2010 and 2015, respectively. His research interests include SBAS, GNSS signal processing and anti-spoofing techniques.

Byung-Hyi Gong is a M.S. candidate with the Department of Electronics Engineering at Chungnam National University in Korea. he received B.S degrees from Chungnam National University, Department of Mathematics in 2017. His research interests include GNSS receiver, anti-spoofing techniques, Beamforming Techniques.

Young-Seok Lee received the B.S. degree in Electronics Engineering from the Chungnam National University, Daejeon, South Korea in 2020. He is currently a M.S. student for communications and signal processing in Electronics Engineering at Chungnam National University, Daejeon, South Korea. His research interests include wireless sensor networks (WSNs), multiple-input multiple-output (MIMO), and Internet of Things (IoT) sensor networks.

Bang Chul Jung received his BS degree with electronics engineering from Ajou University, Suwon, Rep. of Korea, in 2002, and his MS and PhD degrees in electrical and computer engineering from Korea Advanced Institute of Science and Technology (KAIST), Daejeon, Rep. of Korea, in 2004 and 2008, respectively. He was a senior researcher/ research professor with the KAIST Institute for Information Technology Convergence, Daejeon, Rep. of Korea, from 2009 to 2010. From 2010 to 2015, he was a faculty member of Gyeongsang National University, Tongyeong, Rep. of Korea. He is currently a professor with the Department of Electronics Engineering, Chungnam National University, Daejeon, Rep. of Korea. His research interests include wireless communication systems, Internet-of-Things communications, statistical signal processing, information theory, interference management, radio resource management, spectrum sharing techniques, and machine learning.

Sang Jeong Lee is a professor with the Department of Electronics Engineering, Chungnam National University, Korea. He received his B.S., M.S., and Ph.D. degrees from Seoul National University, Korea, in 1979, 1981, and 1987, respectively. His research interests include GNSS receiver design and robust control.

ABSTRACT

In this paper, the performance of several spoofing mitigation techniques using multiple receive antennas is compared and analyzed under various spoofing attack scenarios. We consider three different spoofing attack scenarios in this paper. In the first scenario, the received power of the spoofing signal is 5 dB higher than that of the satellite signal and the spoofing signal has a completely different code phase and doppler frequency from the satellite signal at the GNSS receiver. In the second scenario, the received power of the spoofing signal is 5 dB higher than that of the satellite signal and the spoofing signal has

 https://doi.org/10.33012/2021.17833

0.45 chip delay in the code phase of the satellite signal at the GNSS receiver. In the third scenario, the received power of the spoofing signal is 0-2 dB higher than that of the satellite signal and the spoofing signal has 0.45 chip delay in the code phase of the satellite signal at the GNSS receiver. The uniform circular array consists of 4, 5, or 7 elements. The software-based GPS L1 C / A signal generator and the spoofing signals generator is designed. The software-based GPS receiver for anti-spoofing techniques based on array antenna is also designed. As indicators for performance, the array antenna radiation pattern, the accuracy of DoA estimation, C/N0 after applying the anti-spoofing technique, and code tracking error are used. From the results, it is confirmed that the accuracy of the DoA estimation increases as the number of antennas increases when the received power of the spoofing signal is sufficiently higher than that of the satellite signal. However, the performance of the spoofing mitigation technique becomes deteriorated when the received power of the spoofing signal is similar to that of the satellite signal even though the number of antenna elements is large enough.

INTRODUCTION

GNSS signals are weak and vulnerable to interference. Among intentional interference signals, the spoofing signal has the same structure as the GNSS signal. Due to this characteristics of spoofing signals, spoofing attacks have a more harmful effect on GNSS receivers. Recently, various anti-spoofing techniques have been studied. Anti-spoofing technique can be divided into single antenna based technique and multiple antenna based technique. Anti-spoofing techniques with a single antenna include the signal power level monitoring, Time-of-Arrival (TOA) discrimination, Angle-of-Arrival (AOA) discrimination and Receiver Autonomous Integrity Monitoring (RAIM)[1]. Anti-spoofing techniques based on array antenna are effective for spoofing detection as well as for spoofing mitigation. So, anti-spoofing techniques with array antenna have received much attention from both academia and industry in detecting the spoofing attack and mitigating its effect[2][3][4][5][6][7][8][9]. In most studies, the performance of the anti-spoofing technique was analyzed only when the number of GNSS receive antennas is larger than the number of signals including legitimate satellites and spoofers or the the received signal power of the spoofer is much higher than that of the satellite signal. In practice, however, it is difficult to use an array antenna with many elements due to limited space and complexity and the spoofer may control the transmit power so that the received power of the spoofing signal is similar to that of the satellite signal.

In this paper, the performance of several spoofing mitigation techniques with multiple receive antennas will be compared and analyzed under various spoofing attack scenarios. We consider three different spoofing attack scenarios in this paper. The uniform antenna consists of 4, 5, or 7 elements. For doing this, a software-based GPS L1 C / A signal generator and a spoofing signal generator is designed. A software-based GPS receiver for anti-spoofing techniques based on array antenna is also designed.

GNSS SPOOFING MITIGATION TECHNIQUES BASED ON ARRAY ANTENNA

When a receiver with N array antennas receives M_A satellite signals and M_S spoof signals, the received signal is as follows:

$$\mathrm{r(t)} = \sum_{m=1}^{M_A} a_m^A s_m^A(t) + a^s \sum_{p=1}^{M_s} s_p^s(t) + n(t). \quad (1)$$

where a_m^A is the direction vector of the m-th satellite, and a^s is the direction vector of the spoofing signal. $n(t)$ is the thermal noise added to the received signal, and each element is AWGN (Additive White Gaussian Noise) following a normal distribution with an average of 0 and a variance of σ^2. $s_m^A(t)$ and $s_p^s(t)$ denote satellite signals and spoofing signals, respectively. It is assumed that the spoofing signal transmits several spoof signals from one spoof.

Various studies have been conducted on the spoofing signal mitigation technique using array antennas. This paper compare and analyze three spoofing mitigation techniques in various spoofing attacks environments. The first technique is Maximum Eigenvalue Approximation(MEA). The MEA method using eigenvalue decomposition is the simplest design. The MEA technique using eigenvalue decomposition can be designed in the simplest of the three methods. MEA is a technique that mitigates spoofing signals by forming nulls based on eigenvectors corresponding to the maximum eigenvalues. The covariance of the received signal can be defined as follows:

$$R_r = \mathbb{E}[rr^H] = \frac{1}{N}\sum_{i=1}^{N}[r(iT_s)r^H(iT_s)]. \quad (2)$$

where N means the total number of samples, and T_s means the sampling frequency. Using the covariance defined in (2), the eigenvector of the spoofing signal is estimated through eigenvalue decomposition. A null is formed based on the eigenvector of the spoofing signal estimated. Except for this, the remaining eigenvector matrix is assumed to be the noise subspace P_n. The spoofing signal is mitigated by projecting the received signal onto the estimated noise subspace P_n.

$$\hat{r}(t) = P_n^H r(t) = P_n^H\left(\sum_{m=1}^{M_A} a_m^A s_m^A(t) + a^s \sum_{p=1}^{M_s} s_p^s(t) + n(t)\right) \tag{3}$$

All signals received by the receiver have their own Direction of Arrival (DoA). The accuracy of DoA estimation of the spoofing signal has the greatest influence on the spoofing signal mitigation performance. The most representative algorithm for estimating the DoA of a received signal is Multiple Signal Classification (MUSIC). MUSIC applies eigenvalue decomposition in the same way as MEA and searches for the DoA of the spoofing signal. This algorithm estimates the direction vector for all spaces considering the delay due to the position of the antenna element. This algorithm estimates the DoA of the spoofing signal orthogonal to the signal/noise subspace. It can be estimated by the equation (4).

$$P_{MUSIC}(\theta_i, \phi_j) = \frac{1}{a^H(\theta_i,\phi_j) U_n U_n^H a(\theta_i,\phi_j)} \tag{4}$$

where a means the direction vector of all spaces, θ_i means the search range of the elevation angle, and the range is 0°-90°. ϕ_j means the search range of the azimuth, and the range is 0°-180°. U_n means satellite signal/noise subspace. MUSIC determines the angle at which eq. (4) has the maximum value as the DoA of the spoofing signal. A null space is generated using the result of estimating the direction vector of the spoofing signal, and the equation is expressed as (5).

$$P_n = \mathrm{I} - a(\hat{\theta}, \hat{\phi})\left(a^H(\hat{\theta}, \hat{\phi}) a(\hat{\theta}, \hat{\phi})\right)^{-1} a^H(\hat{\theta}, \hat{\phi}) \tag{5}$$

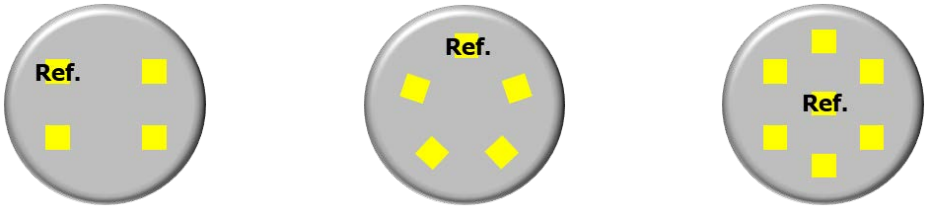
The spoofing signal is mitigated by using the generated null space. The author of [5] designed the C-MUSIC (Cyclic MUSIC) algorithm using the periodicity of satellite signals to estimate the DoA of the spoofing signal. Unlike MUSIC, C-MUSIC uses a Cyclic Autocorrelation Function (CAF) to separate the signal subspace and the noise subspace. The reason for applying CAF is that the effect of noise can be reduced by the characteristics of the periodic signal and cyclostationarity. The satellite signal and the spoofing signal use the same PRN code, whereas the noise is independent over time, so the expected value is statistically zero. CAF is expressed as follows using the received signal model.

$$R_{rr}^{cc} = \mathbb{E}\left[r(nT_s) r^H(nT_s - T_p)\right] = \sum_{m=1}^{M_A} a_m^A \, (a_m^A)^H R_{m^A m^A}^{cc}(T_p) + a^S \left(a^S\right)^H \sum_{p=1}^{M_S} R_{p^s p^s}^{cc}(T_p) + \sum_{m=1}^{M_A} a_i^A \left(a^S\right)^H R_{i^A i^S}^{cc}(T_p) \tag{6}$$

where $R_{m^A m^A}^{cc}(T_p)$ and $R_{p^s p^s}^{cc}(T_p)$ mean the CAF value of the m-th satellite signal and the CAF value of the p-th spoof signal, respectively. Eigenvalue decomposition is performed for the equation defined in equation (6), and the spoofing signal is searched for. C-MUSIC also estimates the direction vector for all spaces considering the delay due to the position of the antenna element. And, it estimates the DoA of the spoofing signal orthogonal to the signal/noise subspace.

SIMULATION APPROACH

The simulation using the array antenna GPS C/A software receiver was performed for a total of three types of array antennas. The types of antennas used in the paper are summarized in fig. 1. The uniform antenna consists of 4, 5, or 7 elements.



(a) 4-element Rectangular (b) 5-elemetn Circular (c) 7-element Circular with center

Fig. 1. Antenna Type for simulation

The software GPS C/A receiver was implemented in MATLAB© and consists of signal acquisition and tracking units. For simulations with software generated signals, IF digital array signals were produced and stored in binary files on a PC using the following settings: RF front end bandwidth of 2 MHz, sampling frequency of 5 MHz, intermediate frequency of 1.4 MHz and Satellite received power of -158 dBW. It generated signals for the three spoofing attack scenarios defined in Table 1.

Table 1. Spoofing attack scenarios with software simulated signals

Scenario ID	Receiver movement	Code delay [chip]	Doppler Frequency [Hz]	Spoofing Signal Received Power [dBW]
1	Fix	N-chip (*N = Integer number)	Random	-153
2	Fix	0.45	< 1 Hz	-153
3	Fix	0.45	< 1 Hz	-158, -156

All scenarios assumed that the receiver was fixed. In the first scenario, the received power of the spoofing signal is 5 dB greater than that of the satellite signal and the spoofing signal has a completely different code phase and doppler frequency from the satellite signal at the GNSS receiver. In the second scenario, the received power of the spoofing signal is 5 dB larger than that of the satellite signal and the spoofing signal has 0.45 chip delay in the code phase of the satellite signal at the GNSS receiver. In the third scenario, the received power of the spoofing signal is 0-2 dB larger than that of the satellite signal and the spoofing signal has 0.45 chip delay in the code phase of the satellite signal at the GNSS receiver.

In order to analyze the performance of the spoofing signal mitigation technique according to the spoofing attacks environment, the simulation environment was configured as shown in Table 2. There are 9 satellite signals, and in order to simulate the actual satellite signal reception environment, a signal was generated by slightly decreasing the received power for a satellite with a low elevation angle. The position of the spoofer was assumed to be 130° in azimuth and 20° in elevation, and spoofing signals were generated targeting satellites received through receiver channels 1-6. In all spoofing attack scenarios, the start time of the anti-spoofing technique is 3 ms after the start of the simulation. The length of the signal generated for each scenario is 500 ms.

Table 2. Simulation Set-up

GPS L1 C/A	# of satellites	9
	Received Power	-158 [dBW]
Spoofing Signal	Position of Spoofer	Azimuth : 130° Elevation : 20°
	Received Power	-153 [dBW]
	# of spoofing signal	6
Algorithm operation start time		3 [ms]
Simulation Time		500 [ms]

SIMULATION RESULTS

Fig. 2 shows the antenna radiation pattern when nulling is performed after MEA, MUSIC, and C-MUSIC techniques are applied in an environment where scenario 1 is applied.

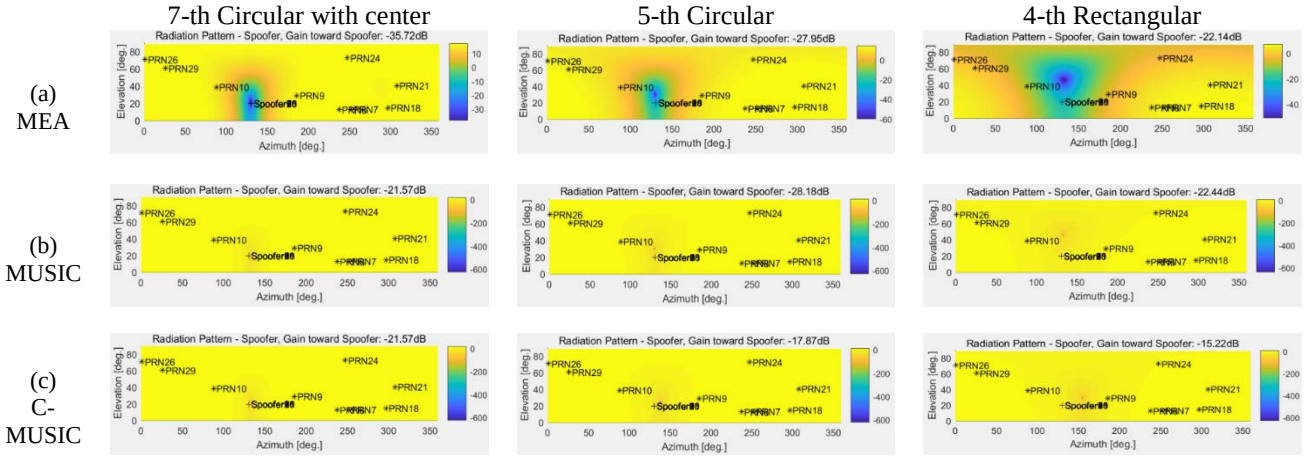


Fig. 2. Antenna Radiation Pattern

From fig. 2, it can be seen that as the number of antenna elements increases, the nulls are formed in a more accurate direction. In addition, more sophisticated and accurate nulls are formed only by applying the DoA estimation algorithm. A more sophisticated and accurate null can be formed when the DoA estimation algorithm is applied, and the satellite signal blocking caused by the null formation can be prevented. The MUSIC algorithm showed that the smaller the antenna element, the lower the estimation accuracy for the elevation angle, and the C-MUSIC algorithm showed that the smaller the antenna element, the lower the estimation accuracy for the azimuth angle. Figs. 3-5 shows the C/N0 and code phase diffrence of PRN 10 after applying the spoofing signal mitigation technique in the same environment. The code phase difference shows the difference in the code phase after the spoofing mitigation and the code phase when the spoof signal does not exist.

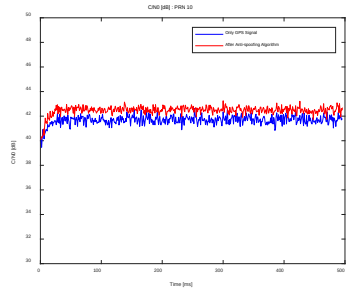
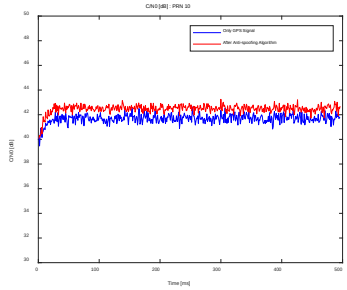
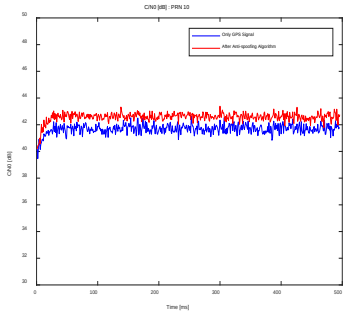
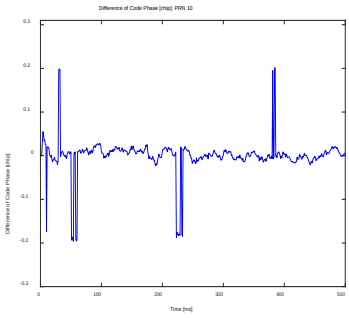
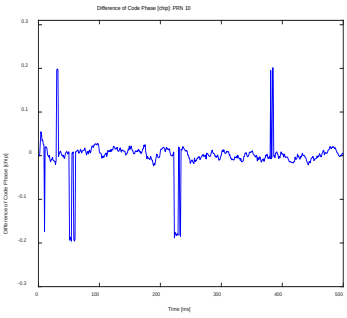
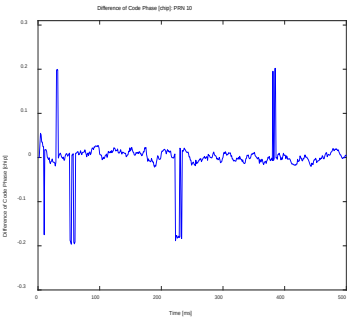
PRN 10			
C/N0			
Difference of Code Phase			
	(a) MEA	(b) MUSIC	(c) C-MUSIC

Fig. 3. C/N0 Estimation - 7 Circular with center

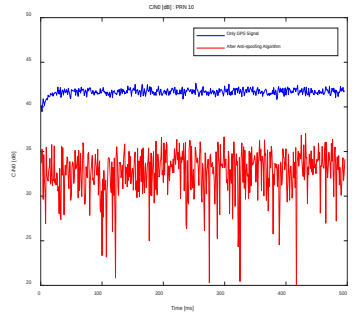
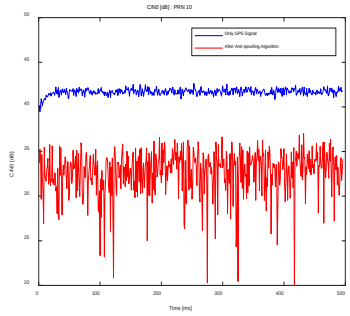
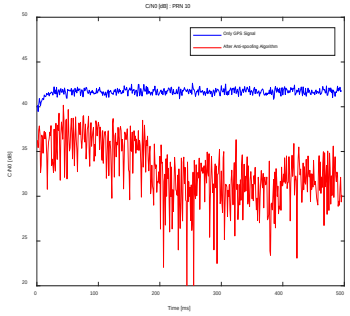
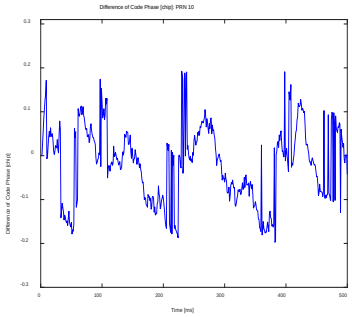
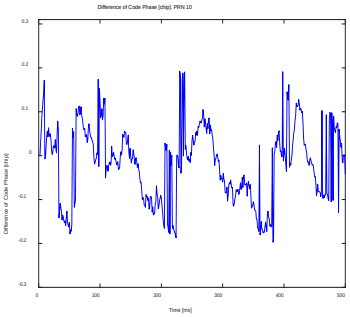
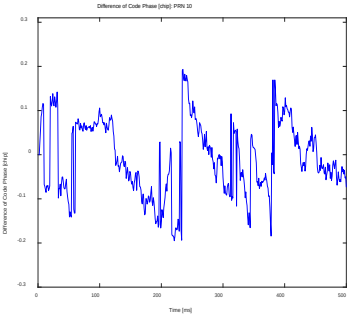
PRN 10			
C/N0			
Difference of Code Phase			
	(a) MEA	(b) MUSIC	(c) C-MUSIC

Fig. 4. C/N0 Estimation - 5 Circular

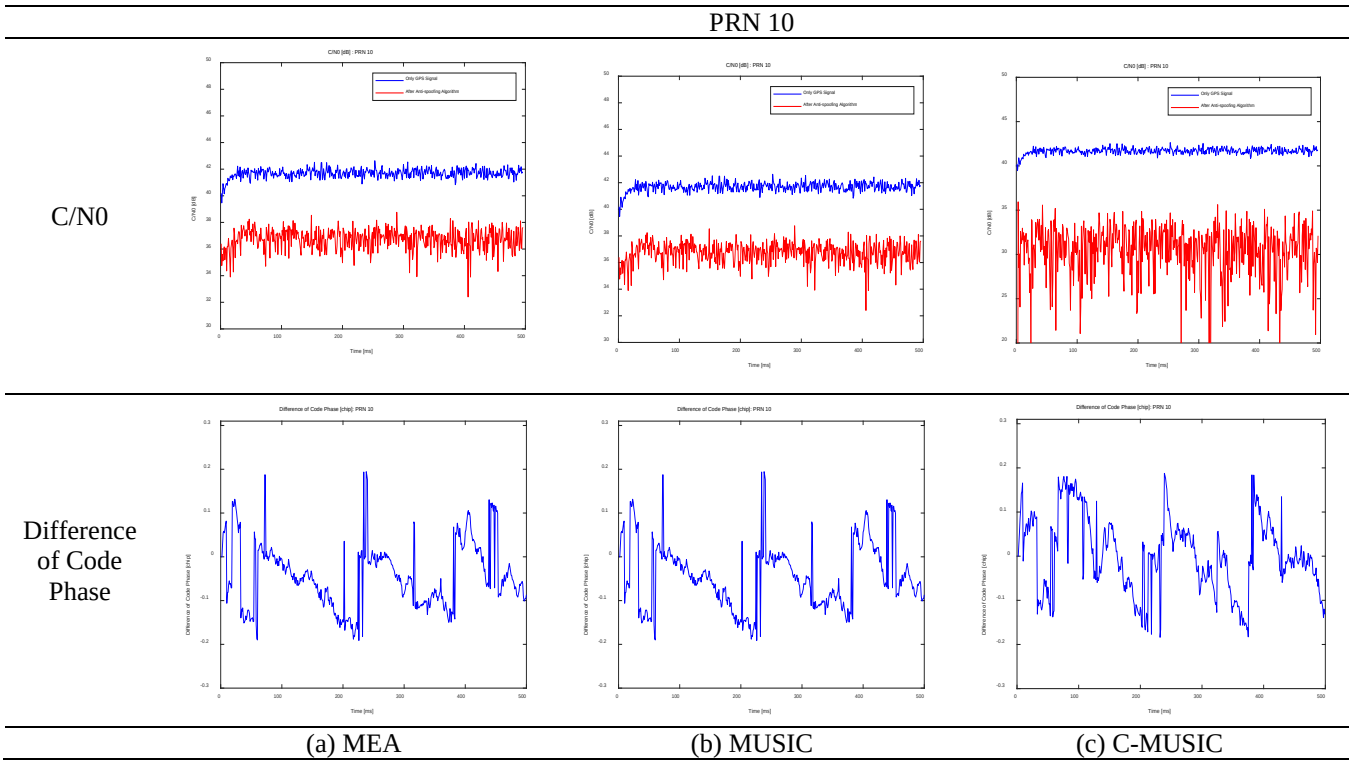


Fig. 5. C/N0 Estimation - 4 Rectangular

From Figure 3-5, it can be seen that as the number of antenna elements decreases, not only the spoofing signal is attenuated, but also the surrounding satellites are attenuated. In the case of a satellite signal affected by attenuation, the C/N0 performance is rapidly degraded, and this effect causes the receiver to not properly estimate the code phase. Fig. 6 shows the antenna radiation pattern when nulling is performed after MEA, MUSIC, and C-MUSIC techniques are applied in an environment where scenario 2 is applied.

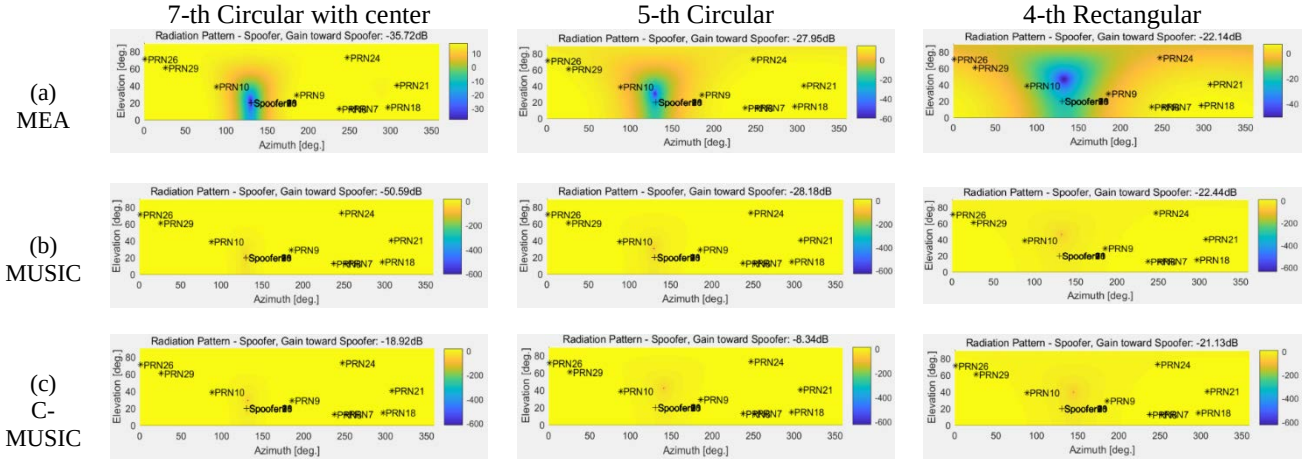


Fig. 6. Antenna Radiation Pattern

Scenario 2 generates the spoofing signal more sophisticated than Scenario 1, and induces the receiver to search for a spoofing signal instead of a satellite signal within a search cell searching for the signal. However, since the DoA estimation algorithm is an algorithm that searches for a physical location of a signal, the mitigation performance is improved when the DoA estimation algorithm is used as in the previous scenario. And, as the number of antenna elements increases, a null is formed in a more

accurate direction. Figs. 7-9 shows the C/N0 and code phase diffrence of PRN 10 after applying the spoofing signal mitigation technique in the same environment.

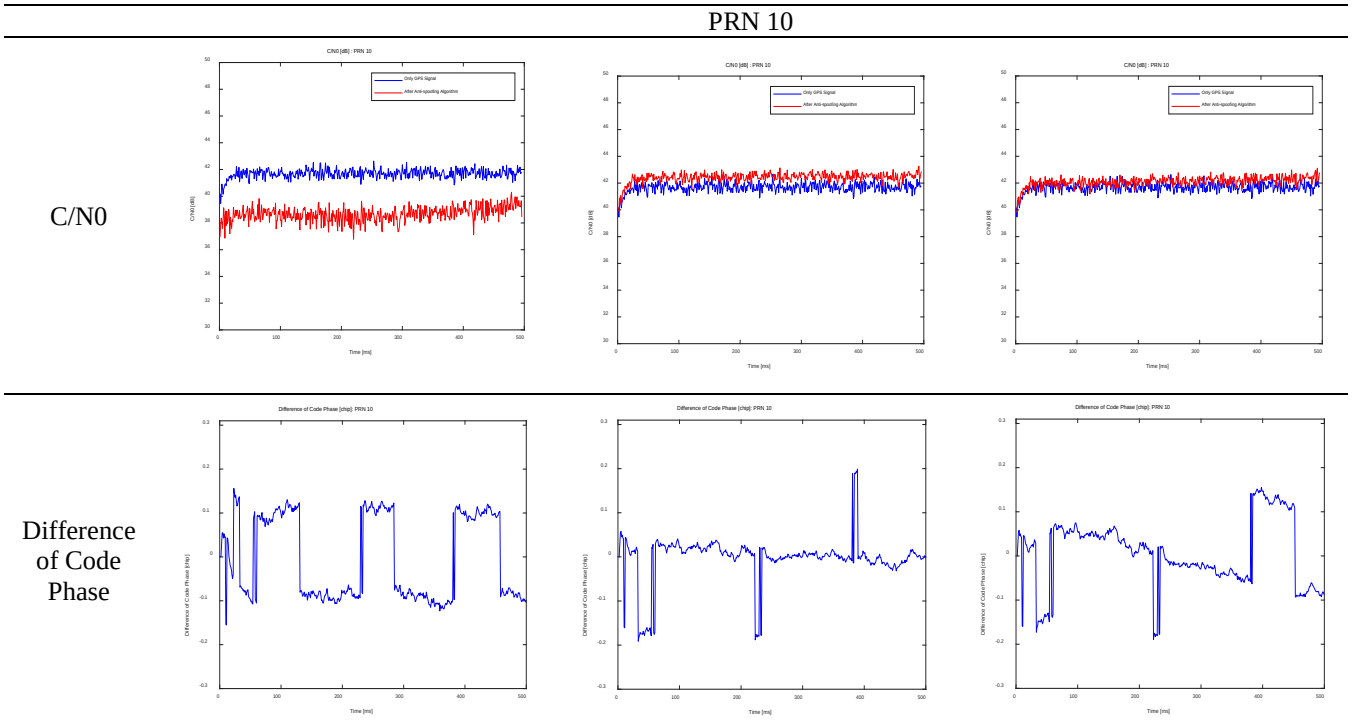


Fig. 7. C/N0 Estimation - 7 Circular with center

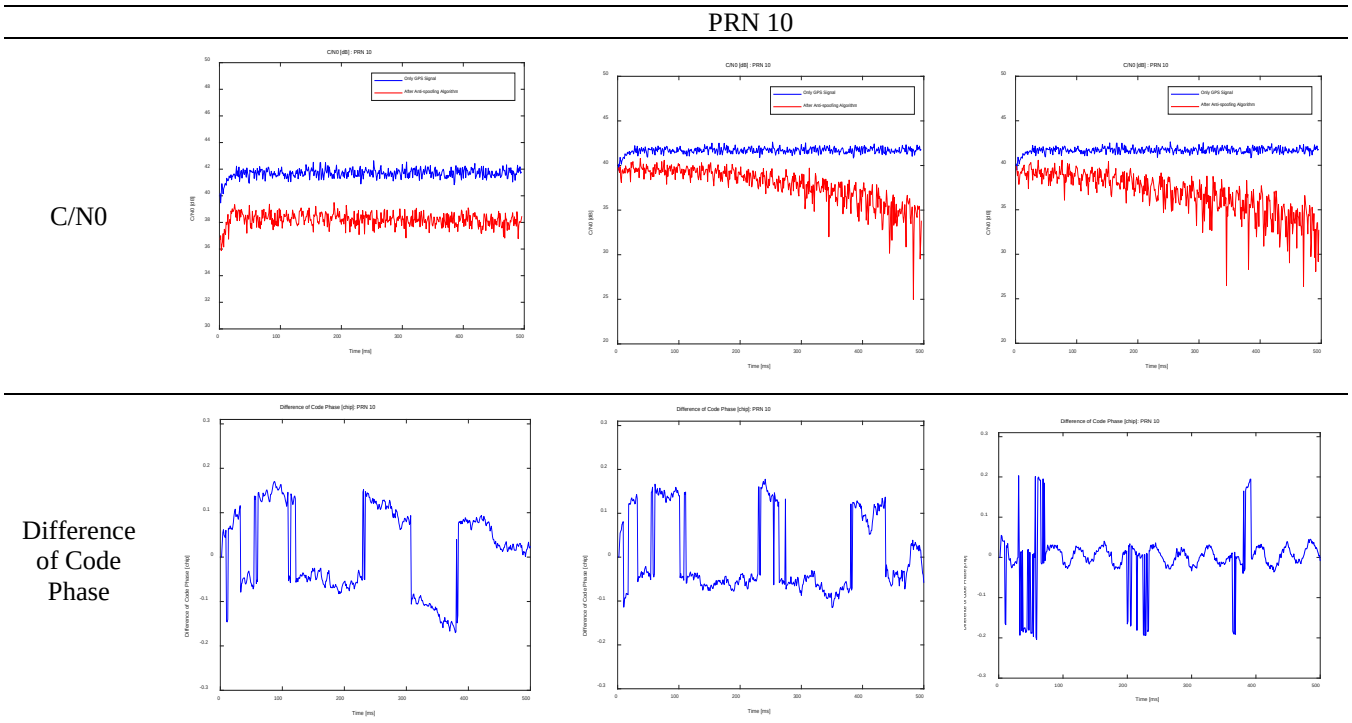


Fig. 8. C/N0 Estimation - 5 Circular

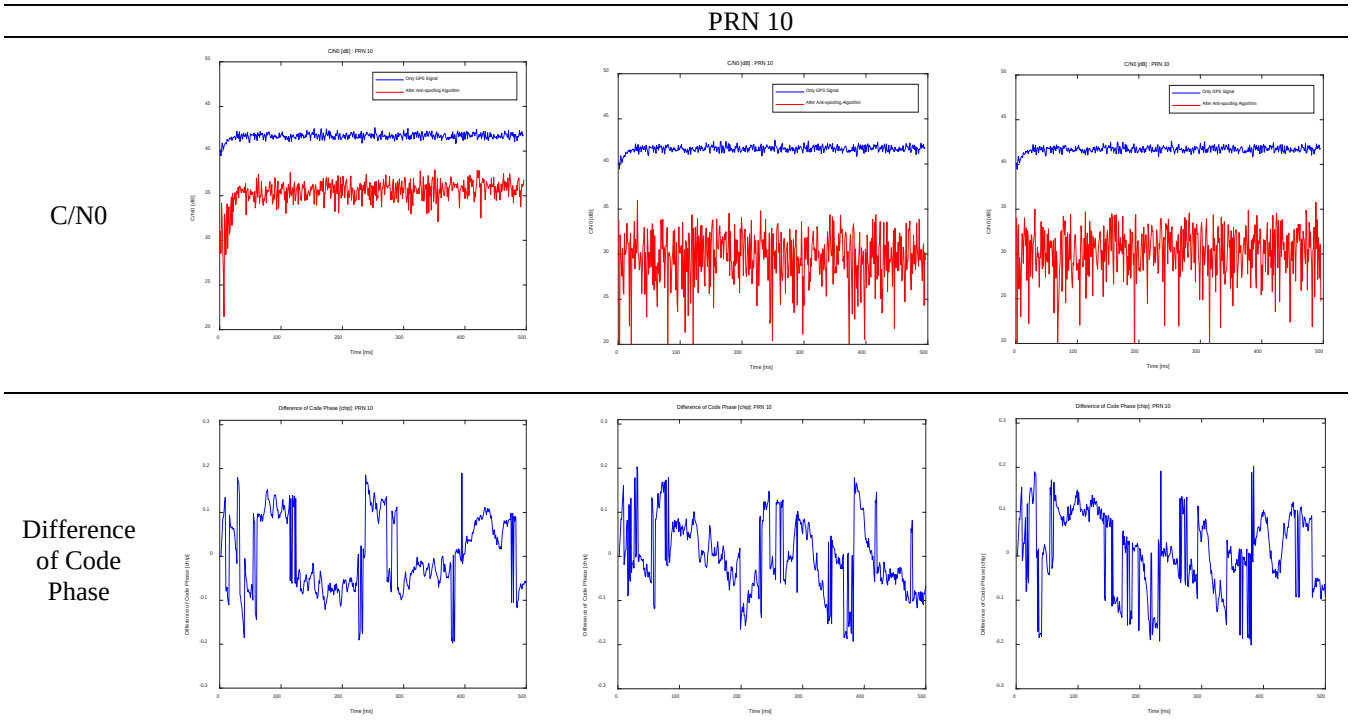


Fig. 9. C/N0 Estimation - 4 Rectangular

From Figure 7-9, it can be seen that as the number of antenna elements decreases, not only the spoofing signal is attenuated, but also the surrounding satellites are attenuated. The PRN 10 satellite, which is located in a similar position to the spoofer, is

affected by the spoofing mitigation technique, so that C/N0 decreases and code phase tracking is not performed properly. In particular, when a 4-th antenna is used, satellite signal reception is impossible. Since the satellite signal before passing through the correlator has a lower power than the noise power, it is difficult to estimate the DoA of the spoofing signal as the number of array antenna elements decreases. Figs. 10-11 show the antenna radiation pattern when nulling is performed after MEA, MUSIC, and C-MUSIC techniques are applied in an environment where scenario 3 is applied. Each figure shows the case where the spoofing signal received power is -158 dBW and -156 dBW.

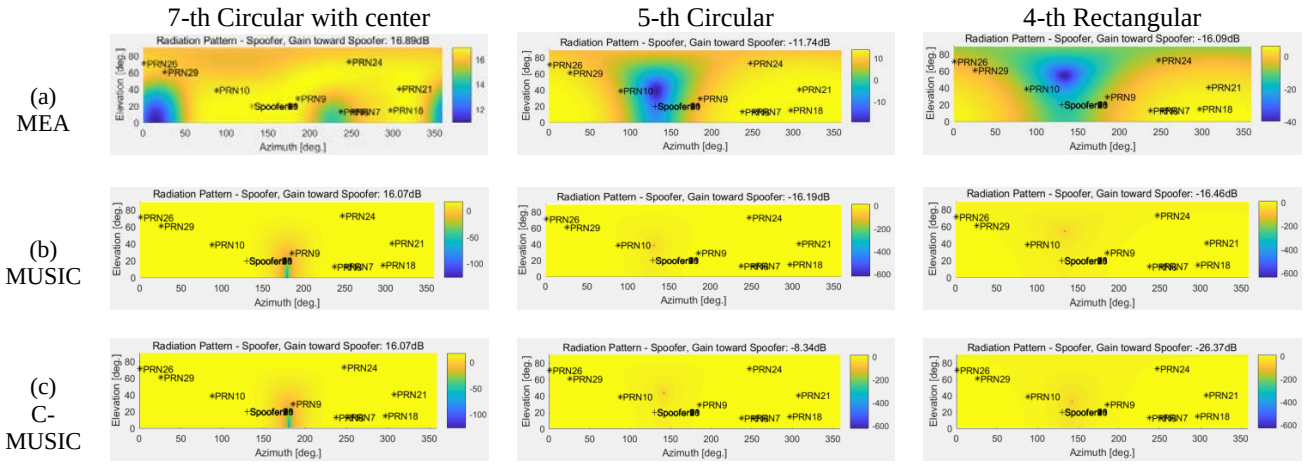


Fig. 10. Antenna Radiation Pattern - Spoofing Signal Received Power : -158 [dBW]

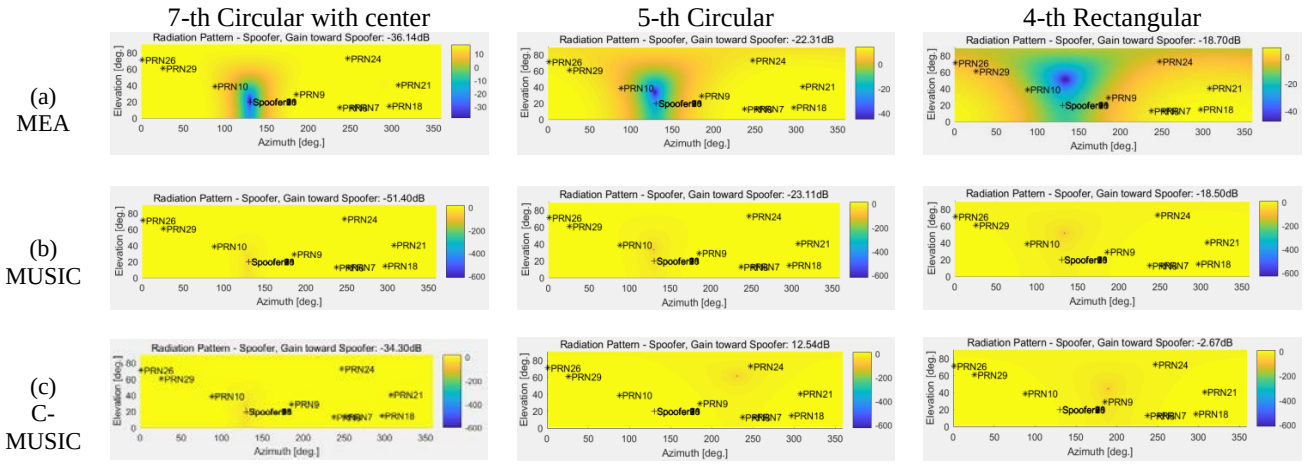


Fig. 11. Antenna Radiation Pattern - Spoofing Signal Received Power : -156 [dBW]

From the results shown in Fig. 10-11, it can be seen that the anti-spoofing algorithm applied before correlation does not perform properly in a situation where the received power of the spoofing signal is similar to that of the satellite signal. When a 4-element antenna is used, the MEA technique shows similar antenna radiation patterns in figs. 10 and 11. This means that when the number of elements of the array antenna is small, it is difficult to mitigate only the spoofing signal unless the received power of the spoofing signal is significantly high. In particular, since the satellite signal before passing through the correlator has a lower power than the noise power, the larger the number of antenna elements is, the more advantageous it is to detect and mitigate the spoofing signal. Figs. 12-14 show the C/N0 and code phase diffrence of PRN 10 after applying the spoofing signal mitigation technique in the same environment.

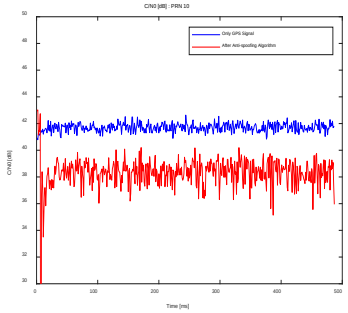
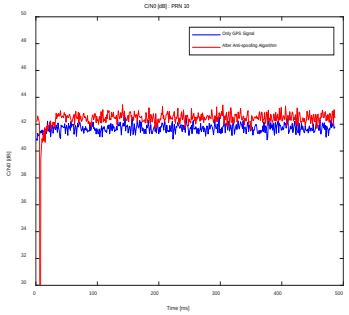
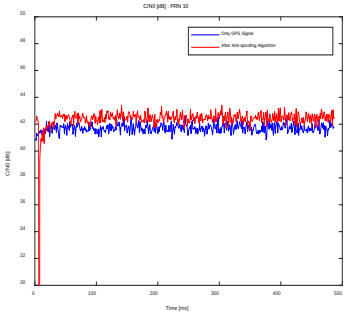
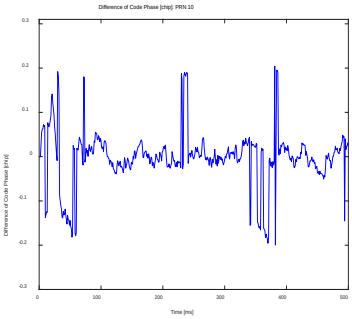
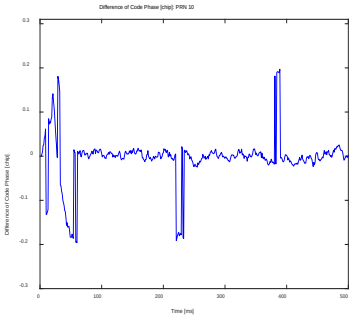
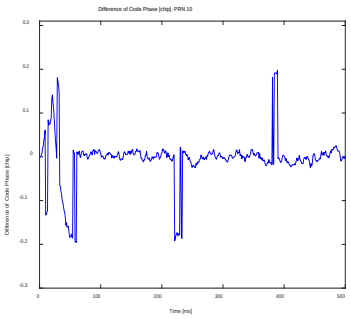
PRN 10			
C/N0			
Difference of Code Phase			
	(a) MEA	(b) MUSIC	(c) C-MUSIC

Fig. 12. C/N0 Estimation - 7 Circular with center

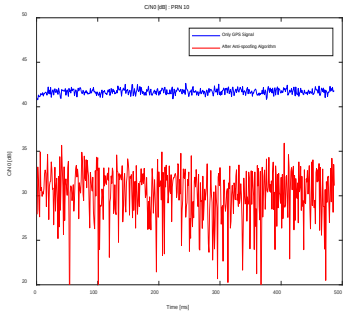
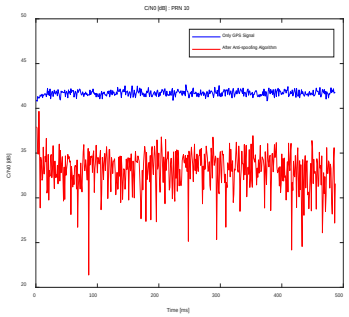
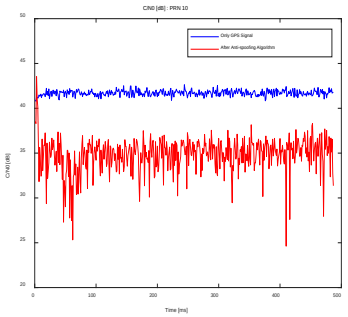
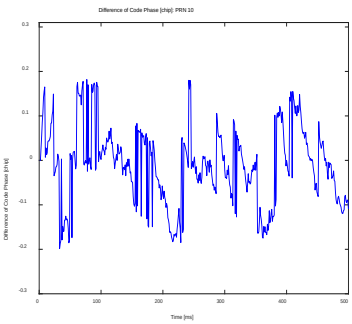
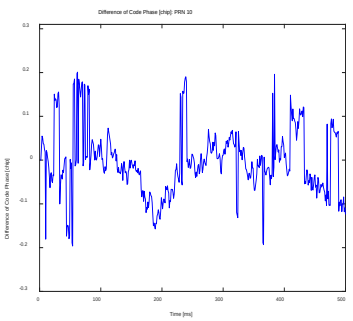
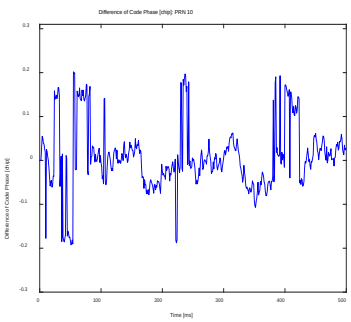
PRN 10			
C/N0			
Difference of Code Phase			
	(a) MEA	(b) MUSIC	(c) C-MUSIC

Fig. 13. C/N0 Estimation - 5 Circular

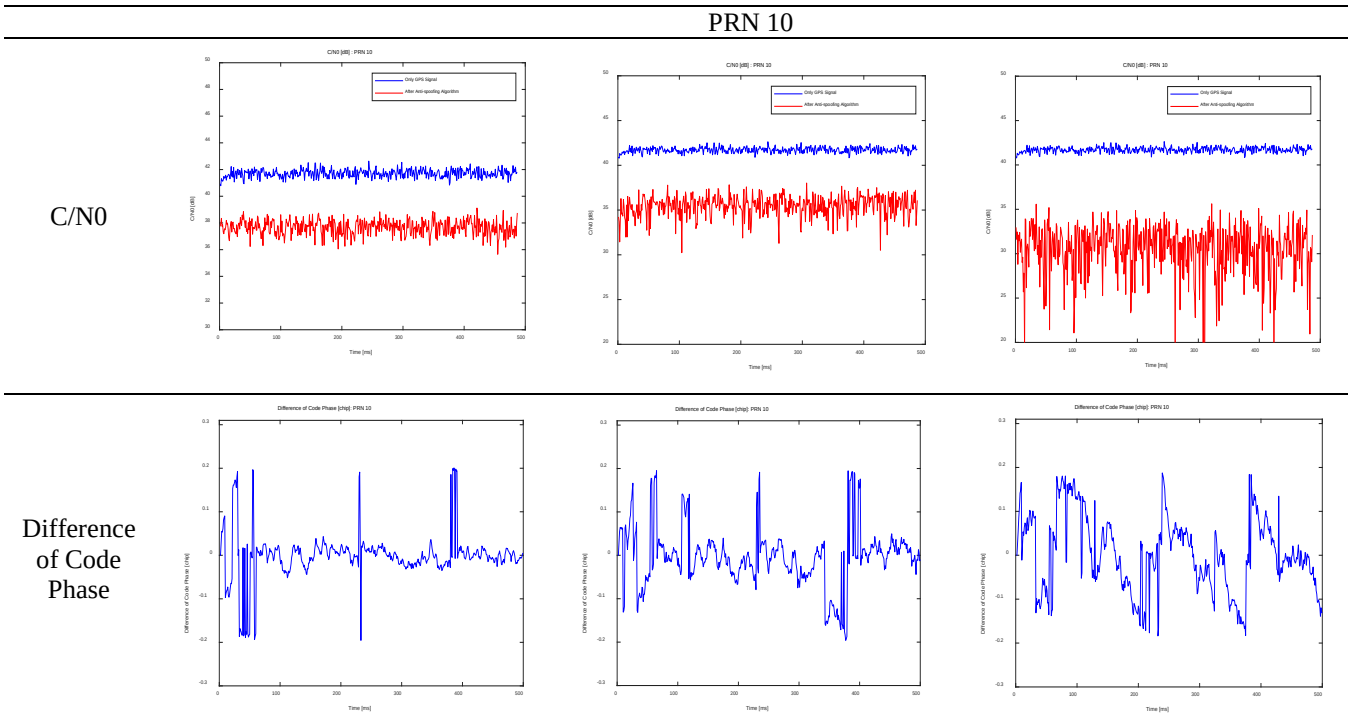


Fig. 14. C/N0 Estimation - 4 Rectangular

From figs. 12-14, it can be seen that in the environment where sophisticated spoofing signals are generated, even if the number of antenna elements increases in the MEA technique, it is difficult to recover the original signal from the satellite signals near the spoof. The case of using a 7-element antenna, the situation where the DoA estimation algorithm was applied was better to recover the original signal. This means that it is necessary to estimate the location of the spoofer in the environment where the sophisticated spoofing signals are generated rather than the simple spoofing attack environment such as Scenario 1.

CONCLUSION

In this paper, the performance of several spoofing mitigation techniques with multiple receive antennas is compared and analyzed under various spoofing attack scenarios. The spoofing signal mitigation techniques analyzed in the paper were applied and analyzed before correlation. In a simple spoofing attack environment such as scenario 1, applying MEA alone without DoA estimation is sufficient to mitigate the spoofing signal. However, in the environment where sophisticated spoofing signals are generated, even if the number of antenna elements increases in the MEA technique, it is difficult to recover the original signal from the satellite signals near the spoof. When the receiver applied the DoA estimation algorithm (MUSIC, C-MUSIC) and used the 7 element antenna, it showed excellent anti-spoofing performance in all spoofing attack scenarios. However, even when the DoA estimation algorithm was used, as the number of antenna elements decreased, the spoofing signal mitigation performance decreased. Since the satellite signal before passing through the correlator has a lower power than the noise power, the larger the number of antenna elements is, the more advantageous it is to detect and mitigate the spoofing signal. In addition, in the case where the received power of the spoofing signal is transmitted equal to the received power of the satellite signal, the use of the received signal before correlation shows that the spoof signal is not properly detected even when using the DoA estimation algorithm. Since the received signal passing through the correlator has a much larger power than the noise power, it is easy to extract the characteristics of the spoofing signal in the same environment. Therefore, it is necessary to study a technique for detecting and mitigation the spoofing signal using the signal after correlation.

REFERENCES

1. Jafarnia-Jahromi, A., Broumandan, A., Nielsen, J., and Lachapelle, G., “GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques,” *International Journal of Navigation and Observation*, Vol. 2012, 2012.
2. Daneshmand, S., Jafarnia-Jahromi, A., Broumandan, A., and Lachapelle, G., “A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array,” *in Proc. the 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012)*, Nashville, TN, September 2012, pp. 1233-1243.
3. Daneshmand, S., Jafarnia-Jahromi, A., Broumandan, A., and Lachapelle, G., "A GNSS structural interference mitigation technique using antenna array processing," *2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM)*, A Coruna, 2014, pp. 109-112
4. Magiera, J., “A Multi-Antenna Scheme for Early Detection and Mitigation of Intermediate GNSS Spoofing,” *MDPI Sensors*, Vol. 19, No. 10, 2019, pp. 2411-2417.
5. Zhang, J., Cui, X., Xu, H., and Lu, M., “A Two-Stage Interference Suppression Scheme Based on Antenna Array for GNSS Jamming and Spoofing,” *MDPI Sensors*, Vol. 19, No. 18, 2019, pp.3870-3895.
6. Montgomery, P. Y., Humphreys, T. E., and Ledvina, B. M., "Receiver-Autonomous Spoofing Detection: Experimental Results of a Multi-Antenna Receiver Defense against a Portable Civil GPS Spoofer," *in Proc. the 2009 International Technical Meeting of The Institute of Navigation*, Anaheim, CA, January 2009, pp. 124-130.
7. Daneshmand, S., Jafarnia-Jahromi, A., Broumandan, A., and Lachapelle, G., " GNSS Spoofing Mitigation in Multipath Environments Using Space-Time Processing," *in Proc. the European Navigation Conference*, Vienna, Austria, 2013, pp. 23-25
8. Magiera, J., and Katulski, R., “ Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing,” *Journal of Applied Research and Technology*, Vol. 13, No. 1, 2015, pp. 45-47.
9. Appel, M., Konovaltsev, A., and Meurer, M., “Robust Spoofing Detection and Mitigation based on Direction of Arrival Estimation,” *in Proc. the 28th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2015)*, Tampa, Florida, September 2015, pp. 3335-3344.